

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-212458

(43)Date of publication of application : 06.08.1999

(51)Int.Cl. G09C 1/00
G09C 1/00
G09C 1/00
H04L 9/30

(21)Application number : 10-013748

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 27.01.1998

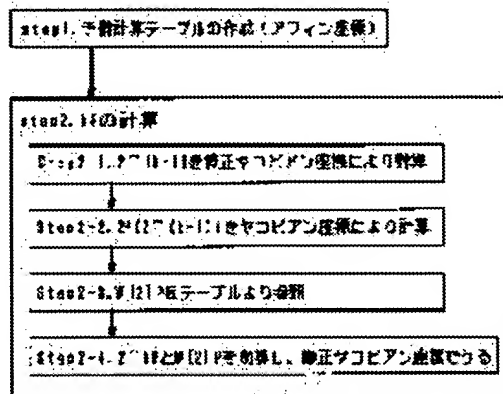
(72)Inventor : MIYAJI MITSUKO
ONO TAKATOSHI

(54) ELLIPTIC CURVE OPERATION DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an elliptic curve operation device in a quick cipher and signature system.

SOLUTION: In an auxiliary calculation table generation step 1, an auxiliary calculation table is generated with affine coordinates. In a kP calculation step 2, kP is obtained by mixture coordinates where addition to values (affine coordinates) of the auxiliary calculation table is obtained in revised Jacobian coordinates and the result is multiplied by power of two in correction Jacobian coordinates but the final result is obtained in Jacobian coordinates. Mixture coordinates and revised Jacobian coordinates are used to reduce the number of multiplications.



LEGAL STATUS

[Date of request for examination]

19.01.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration].

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

THIS PAGE BLANK (USPTO)

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C) 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-212458

(43) 公開日 平成11年(1999) 8月6日

(51) Int.Cl.⁶

G 0 9 C 1/00

H 0 4 L 9/30

識別記号

6 5 0

6 2 0

6 4 0

F I

G 0 9 C 1/00

H 0 4 L 9/00

6 5 0 Z

6 2 0 Z

6 4 0 B

6 6 3 Z

審査請求 未請求 請求項の数10 O L (全 9 頁)

(21) 出願番号 特願平10-13748

(22) 出願日 平成10年(1998) 1月27日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 宮地 充子

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 小野 貴敏

愛知県名古屋市中区栄2丁目6番1号白川
ビル別館5階 株式会社松下電器情報シス
テム名古屋研究所内

(74) 代理人 弁理士 滝本 智之 (外1名)

(54) 【発明の名称】 楕円曲線演算装置

(57) 【要約】

【課題】 高速な暗号及び署名方式における楕円曲線の演算装置を提供する。

【解決手段】 (1) 予備計算テーブル作成
アフィン座標で予備計算テーブルを作成する。

(2) kP の計算

予備計算テーブルの値(アフィン座標)との加算を修正ヤコビアン座標で求めて、その結果を修正ヤコビアン座標で2乗倍するが、最終結果はヤコビアン座標で得るといふ混合座標によりkPを求める。混合座標と修正ヤコビアン座標を利用することで、乗算全体の回数を削減することを特徴とする楕円曲線演算装置を構成する。

step1. 予備計算テーブルの作成 (アフィン座標)

step2. kP の計算

Step2-1. $2^{-(k-1)}$ を修正ヤコビアン座標により計算

Step2-2. $2^k (2^{-(k-1)})$ をヤコビアン座標により計算

Step2-3. W[2] P をテーブルより参照

Step2-4. $2^{-k} P$ と W[2] P を加算し、修正ヤコビアン座標でうる

【特許請求の範囲】

【請求項 1】 p を素数とし、有限体 $GF(p)$ 上の楕円曲線を $E: y^2 = x^3 + ax + b$ とし、 $E(GF(p))$ の元 $P = (x, y)$ を $Z=1$, $X=x*Z^2$, $Y=y*Z^3$ により変換した射影座標 (X, Y, Z) において、加算公式の内部点を修正ヤコビアン座標 $(X, Y, Z, a*Z^4)$ ともつことを特徴とする楕円曲線演算装置。

【請求項 2】 p を素数とし、 r を正整数とするとき、有限体 $GF(p^r)$ 上の楕円曲線を E とし、 $E(GF(p^r))$ の元を $P = (x, y)$ を $Z=1$, $X=x*Z^2$, $Y=y*Z^3$ により変換した射影座標 (X, Y, Z) において、加算公式の内部点を修正ヤコビアン座標 $(X, Y, Z, a*Z^4)$ ともつことを特徴とする楕円曲線演算装置。

【請求項 3】 上記楕円曲線演算装置において、 $E(GF(p))$ の元を修正ヤコビアン座標 $P=(X1, Y1, Z1, a*Z1^4)$, $Q=(X2, Y2, Z2, a*Z2^4)$ ($P \neq Q$)

で表すとき、 $P+Q=R=(X3, Y3, Z3, a*Z3^4)$ を、
 $U1=X1*Z2^2$, $U2=X2*Z1^2$, $S1=Y1*Z2^3$, $S2=Y2*Z1^3$, $H=U2-U1$, $r=S2-S1$

を計算し、

$$X3 = -H^3 - 2U1*H^2 + r^2,$$

$$Y3 = -S1*H^3 + r(U1*H^2 - X3),$$

$$Z3 = Z1*Z2*H,$$

$$a*Z3^4 = a(Z3^2)^2$$

により求めることを特徴とした請求項 1 記載の楕円曲線演算装置。

【請求項 4】 上記楕円曲線演算装置において、 $E(GF(p))$ の元を、修正ヤコビアン座標

$$P=(X1, Y1, Z1, a*Z1^4)$$

とするとき、 $2P=R=(X3, Y3, Z3, a*Z3^4)$ を、

$$S=4X1*Y1^2, M=3X1^2+a*Z1^4, T=-2S+M^2$$

を計算し、

$$X3 = T,$$

$$Y3 = -8Y1^4 + M(S-T),$$

$$Z3 = 2Y1*Z1,$$

$$a*Z3^4 = 2^4*(Y1^4)*(a*Z1^4)$$

により求めることを特徴とした請求項 1 記載の楕円曲線演算装置。

【請求項 5】 p を素数とし、 k を正整数とするとき、有限体 $GF(p)$ 上の楕円曲線を

$$E: y^2 = x^3 + ax + b$$

とし、 $E(GF(p))$ の元 $P = (x, y)$ の幕倍点 $kP = P + \dots + P$ (k 回の加算) の計算を、座標を 2 個以上組み合わせて行なうことを特徴とした楕円曲線演算装置。

【請求項 6】 p を素数とし、 r, k を正整数とし、有限体 $GF(p^r)$ 上の楕円曲線を E とし、 $E(GF(p^r))$ の元 $P = (x, y)$ の幕倍点 $kP = P + \dots + P$ (k 回の加算) の計算を、座標を 2 個以上組み合わせて行なうことを特徴とした楕円曲線演算装置。

【請求項 7】 p を素数、 k を正整数、有限体 $GF(p)$ 上の楕円曲線を $E: y^2 = x^3 + ax + b$ とし、

$E(GF(p))$ の元 $P = (x, y)$ の幕倍点 $kP = P + \dots + P$ (k 回の加算)

を計算する上記楕円曲線演算装置において、 w を正整数とし、 k を

$$k=2^k0(2^k1(\dots(2^kvW[v]+W[v-1])\dots)+W[0])$$

($W[i]$ は奇数、かつ $1 \leq W[i] \leq 2^w-1$) と表すとき、テーブル

$$iP = Pi=(xi, yi) \quad (i \text{ は奇数, かつ } 1 \leq i \leq 2^w-1)$$

をアフィン座標で計算し、 kP の計算を、 $(ki-1)$ 回の 2 倍点の計算は、請求項 1 記載の座標 $(X, Y, Z, a*Z^4)$ で行い、 ki 回目の 2 倍点の結果は、ヤコビアン座標 (X, Y, Z) で求め、 (X, Y, Z) とテーブルの点 Pi との加算は、請求項 1 記載の座標 $(X, Y, Z, a*Z^4)$ で求めることを、繰り返すことによって得ることを特徴とした請求項 5 記載の楕円曲線演算装置。

【請求項 8】 p を素数、 k を正整数、有限体 $GF(p)$ 上の楕円曲線を $E: y^2 = x^3 + ax + b$ とし、

$E(GF(p))$ の元 $P = (x, y)$ の幕倍点 $kP = P + \dots + P$ (k 回の加算)

を計算する上記楕円曲線演算装置において、 w を正整数とし、 k を

$$k=2^k0(2^k1(\dots(2^kvW[v]+W[v-1])\dots)+W[0])$$

($W[i]$ は奇数、かつ $1 \leq W[i] \leq 2^w-1$) と表すとき、テーブル

$$iP = Pi=(Xi, Yi, Zi, Zi^2, Zi^3) \quad (i \text{ は奇数, かつ } 1 \leq i \leq 2^w-1)$$

をチャドノブスキヤコビアン座標で求め、 kP の計算を、 $(ki-1)$ 回の 2 倍点の計算は、請求項 1 記載の修正ヤコビアン座標 $(X, Y, Z, a*Z^4)$ で行い、 ki 回目の 2 倍点の結果は、ヤコビアン座標 (X, Y, Z) で求め、 (X, Y, Z) とテーブルの点 Pi との加算は、請求項 1 記載の修正ヤコビアン座標 $(X, Y, Z, a*Z^4)$ で求めることを、繰り返すことによって得ることを特徴とした請求項 5 記載の楕円曲線演算装置。

【請求項 9】 p を素数、 k を正整数、有限体 $GF(p)$ 上の楕円曲線を $E: y^2 = x^3 + ax + b$ とし、

$E(GF(p))$ の元 $P = (x, y)$ の幕倍点 $kP = P + \dots + P$ (k 回の加算)

を計算する上記楕円曲線演算装置において、 w を正整数とし、 k を

$$k=2^k0(2^k1(\dots(2^kvW[v]+W[v-1])\dots)+W[0])$$

($W[i]$ は奇数、かつ $1 \leq W[i] \leq 2^w-1$) と表すとき、テーブル

$$iP = Pi=(Xi, Yi, Zi, Zi^2, Zi^3)$$

(i は奇数、かつ $1 \leq i \leq 2^w-1$) をチャドノブスキヤコビアン座標で求めるとき、はじめに、 $2P=(x, y)$ をアフィン座標で求めることを特徴とした請求項 8 記載の楕円曲線演算装置。

【請求項 10】 p を素数、 k を正整数、有限体 $GF(p)$ 上の楕円曲線を $E: y^2 = x^3 + ax + b$ とし、

$E(GF(p))$ の元 $P = (x, y)$ の冪倍点 $kP = P + \dots + P$ (k 回の加算)

を計算する上記楕円曲線演算装置において、 w を正整数とし、 k を

$$k = 2^k 0 (2^{k_1} (\dots (2^{k_v} w[v] + w[v-1]) \dots) + w[0])$$

($w[i]$ は奇数、かつ $1 \leq w[i] \leq 2^{w-1}$) と表すとき、

テーブル

$$iP = Pi = (Xi, Yi, Zi, Zi^2, Zi^3)$$

(i は奇数、かつ $1 \leq i \leq 2^{w-1}$) をチャドノブスキヤコピアン座標で求めるとき、はじめに、 $2P = (x, y)$ をチャドノブスキヤコピアン座標で求めることを特徴とした請求項 8 記載の楕円曲線演算装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は情報セキュリティ技術としての暗号技術に関するものであり、特に、楕円曲線を用いて実現する暗号及びデジタル署名技術に関するものである。

【0002】

【従来の技術】 秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。この署名方式には公開鍵暗号とよばれる暗号方式を用いる。公開鍵暗号は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。簡単に説明すると、これは暗号化鍵と復号化鍵が異なり、復号化鍵は秘密にするが、暗号化鍵を公開する方式である。この公開鍵暗号の安全性の根拠に用いられるものに離散対数問題がある。離散対数問題には代表的に、有限体上定義されるもの及び楕円曲線上定義されるものがある。これはニールコブリッツ著 "ア コウス イン ナンバア セオリイ アンド クリプトグラフィ" (Neal Koblitz, "A Course in Number theory and Cryptography", Springer-Verlag, 1987) に詳しく述べられている。楕円曲線上の離散対数問題を以下に述べる。

【0003】 楕円曲線上の離散対数問題

$E(GF(p))$ を有限体 $GF(p)$ 上定義された楕円曲線 E とし、 E の位数が大きな素数で割れる元 G をベースポイントとする。このとき、 E の与えられた元 Y に対して、 $Y = xG$

となる整数 x が存在するならば x を求めよ。

【0004】 以下に上記楕円曲線上の離散対数問題を応用したエルガマル署名をまず述べる。

【0005】 (従来例 1) 図 6 は従来例である楕円曲線上のエルガマル署名方式の構成をしめすものである。

【0006】 以下同図を参照しながら従来例の手順を説明する。

(1) センタの設定

p を素数、 $GF(p)$ 上の楕円曲線を E とし、その素数位数 q の元を G とする。ユーザ A の公開鍵を $Y_a = x_a G$ とし、秘密鍵を x_a とする。センターは素数 p 及び楕円曲線 E 及びベースポイント G をシステムパラメータとして公開するとともに、 A の公開鍵 Y_a を公開する。

【0007】 (2) 署名生成

1 乱数 k を生成する。

【0008】 2 $R_1 = kG = (r_x, r_y)$

$s_k = m + r_x x_a \pmod{q}$ を計算する

3 (R_1, s) を署名として m とともに送信する。

【0009】 (3) 署名検証

$$s_1 = mG + r_x Y_a$$

が成り立つかチェックする。

【0010】 上記従来例 1 でわかるように、楕円曲線を用いた署名方式では、固定点 G の冪倍の演算 kG 及び任意点 P (従来例では公開鍵 Y_a に相当) の冪倍の演算 kP_a の計算が必要である。このうち、固定点の演算は、以下の文献に知られるように、予めテーブルを用意しておくことが可能なので、高速に実現できる。

【0011】 E. F. Brickell, D. M. Gordon, K. S. McCurley and D. B. Wilson "Fast exponentiation with pre computation", Advances in cryptology-proceedings of Eurocrypt'92, Lecture notes in computer science, 1993, Springer-verlag, 200-207. 一方、任意点 P の冪倍を計算する方法であるが、これは以下の文献が詳しい。

【0012】 Miyaji, Ono, and Cohen, "Efficient elliptic curve exponentiation", Advances in cryptology-proceedings of ICICS'97, Lecture notes in computer science, 1997, Springer-verlag, 282-290. ここで簡単に、この従来例について説明する。

【0013】 図 7 は従来例である楕円曲線演算装置の構成を示すものである。以下同図を参照しながら従来例の手順を説明する。

【0014】 (従来例 2) p を 160 ビットの素数とし、有限体 $GF(p)$ 上の楕円曲線を E とし、 $E(GF(p))$ の任意の元 P に対して、 $k \cdot P$ の計算をする。ここで、 k の 2 進表現を、

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \dots + k_{159} \cdot 2^{159} = [k_{159}, \dots, k_2, k_1, k_0]$$

($k_0, \dots, k_{159} = 0, 1$) とする。

【0015】 step1. ウィンドウ幅 $w=4$ をもつ addition-subtraction 表現への変換

$$k = 2^k 0 (2^{k_1} (\dots (2^{k_v} w[v] + w[v-1]) \dots) + w[0])$$

ここで、 $w[i]$ は奇数、かつ $1 \leq w[i] \leq 2^{4-i}$ である。

【0016】 $w[i]$ への変換方法は、奇数 $0 \leq t \leq 2^{5-i} - 1$ を $-2^{4-i} \leq t \leq 2^{4-i}$ に変換する自然な変換で

ある。

【0017】step2. 予備計算テーブルの作成
 $sP(s=3, 5, \dots, 15)$ をヤコビアン座標で計算し、予備計算テーブルとする。

【0018】step3. kP の計算
 T を上位ビットより探索し、ウインドウがある毎に、予備計算テーブルの値との加算をヤコビアン座標で求めて、その結果をヤコビアン座標で2乗倍することを繰り返す。

【0019】従来例では、一つの座標を利用するため全体の乗算回数が多くなるという問題がある。

【0020】トータルの計算量を乗算回数で表すと、1882Mul になる。ここで、Mul は1回のGF(p)での乗算を表す。任意点の乗倍点の演算は、2倍点の演算が加算に比べて数多く必要になる。ところが、従来利用されていたプロジェクトブ座標、ヤコビアン座標、チャドノブスキヤコビアン座標の2倍点は、必要な乗算回数が多いので、 kP の計算の全体の計算量が大きくなるという問題がある。

【0021】

【発明が解決しようとする課題】楕円曲線を用いた暗号方式や署名方式では、固定点の乗倍点や任意点の乗倍点を求める楕円曲線演算装置が必須である。特に、任意点の乗倍点の演算には、時間がかかるので、これを高速に行なう研究がされている。

【0022】従来例の乗倍点を求める方法は、各座標系を用いた際のトータルの計算量が最も小さくなる座標を一つだけ利用する方法で、トータルの乗算回数が多いという欠点がある。

【0023】本発明は、この従来例における問題点を鑑みて行なわれたもので、楕円曲線の加算、2倍点の計算時間を鑑みて、楕円曲線演算装置を構成し、これにより高速な暗号及び署名方式を提供することを目的とする。

【0024】

【課題を解決するための手段】本発明は上述の問題点を解決するため、請求項1では p を素数とし、有限体GF(p)上の楕円曲線を $E: y^2 = x^3 + ax + b$ とし、 $E(GF(p))$ の元を $P = (x, y)$ を $Z=1$, $X=x*Z^2$, $Y=y*Z^3$ により変換した射影座標 (X, Y, Z) において、加算公式の内部点を修正ヤコビアンを特徴とする楕円曲線演算装置としている。

【0025】請求項2では、 p を素数とし、 r を正整数とすると、有限体GF(p^r)上の楕円曲線を E とし、 $E(GF(p^r))$ の元を

$$P = (x, y) \text{ を } Z=1, X=x*Z^2, Y=y*Z^3$$

により変換した射影座標 (X, Y, Z) において、加算公式の内部点を修正ヤコビアンを特徴とする楕円曲線演算装置としている。

【0026】請求項3では、上記楕円曲線演算装置において、 $E(GF(p))$ の元を修正ヤコビアン座標

$$P=(X1, Y1, Z1, a*Z1^4), Q=(X2, Y2, Z2, a*Z2^4) \quad (P \neq Q)$$

で表すとき、 $P+Q=R=(X3, Y3, Z3, a*Z3^4)$ を、
 $U1=X1*Z2^2, U2=X2*Z1^2, S1=Y1*Z2^3, S2=Y2*Z1^3, H=U2-U1, r=S2-S1$

を計算し、

$$X3 = -H^3 - 2U1*H^2 + r^2,$$

$$Y3 = -S1*H^3 + r(U1*H^2 - X3),$$

$$Z3 = Z1*Z2*H,$$

$$a*Z3^4 = a(Z3^2)^2$$

により求めることを特徴とした請求項1記載の楕円曲線演算装置としている。

【0027】請求項4では、上記楕円曲線演算装置において、 $E(GF(p))$ の元を、修正ヤコビアン座標

$$P=(X1, Y1, Z1, a*Z1^4)$$

とすると、 $2P=R=(X3, Y3, Z3, a*Z3^4)$ を、

$$S=4X1*Y1^2, M=3X1^2+a*Z1^4, T=-2S+M^2$$

を計算し、

$$X3 = T,$$

$$Y3 = -8Y1^4 + M(S-T),$$

$$Z3 = 2Y1*Z1,$$

$$a*Z3^4 = 2^4*(Y1^4)*(a*Z1^4)$$

により求めることを特徴とした請求項1記載の楕円曲線演算装置としている。

【0028】請求項5では、 p を素数とし、 k を正整数とすると、有限体GF(p)上の楕円曲線を

$$E: y^2 = x^3 + ax + b$$

とし、

$$E(GF(p)) \text{ の元 } P = (x, y) \text{ の乗倍点 } kP = P + \dots + P \quad (k \text{ 回の加算})$$

の計算を、座標を2個以上組み合わせて行なうことを特徴とした楕円曲線演算装置を特徴とする楕円曲線演算装置としている。

【0029】請求項6では、 p を素数とし、 r, k を正整数とし、有限体GF(p^r)上の楕円曲線を E とし、 $E(GF(p^r))$ の元 $P = (x, y)$ の乗倍点 $kP = P + \dots + P$ (k 回の加算)の計算を、座標を2個以上組み合わせて行なうことを特徴とした楕円曲線演算装置としている。

【0030】請求項7では、 p を素数、 k を正整数、有限体GF(p)上の楕円曲線を $E: y^2 = x^3 + ax + b$ とし、

$$E(GF(p)) \text{ の元 } P = (x, y) \text{ の乗倍点 } kP = P + \dots + P \quad (k \text{ 回の加算})$$

を計算する上記楕円曲線演算装置において、 w を正整数とし、 k を

$$k=2^k0(2^k1(\dots(2^kvW[v]+W[v-1])\dots)+W[0])$$

($W[i]$ は奇数、かつ $1 \leq W[i] \leq 2^{w-1}$) と表すとき、テーブル

$$iP = Pi=(xi, yi) \quad (i \text{ は奇数、かつ } 1 \leq i \leq 2^{w-1})$$

をアフィン座標で計算し、 kP の計算を、 $(ki-1)$ 回の2倍点の計算は、請求項1記載の座標 $(X, Y, Z, a*Z^4)$

で行い、 k_i 回目の2倍点の結果は、ヤコビアン座標 (X, Y, Z) で求め、 (X, Y, Z) とテーブルの点 P_i との加算は、請求項1記載の座標 $(X, Y, Z, a*Z^4)$ で求めることを、繰り返すことによって得ることを特徴とした請求項5記載の楕円曲線演算装置としている。

【0031】請求項8では、 p を素数、 k を正整数、有限体 $GF(p)$ 上の楕円曲線を

$$E: y^2 = x^3 + ax + b$$

とし、 $E(GF(p))$ の元 $P = (x, y)$ の冪倍点 $kP = P + \dots + P$ (k 回の加算) を計算する上記楕円曲線演算装置

において、 w を正整数とし、 k を

$$k = 2^k0(2^k1(\dots(2^kwW[v] + W[v-1]) \dots) + W[0])$$

($W[i]$ は奇数、かつ $1 \leq W[i] \leq 2^w-1$) と表すとき、

テーブル

$$iP = P_i = (X_i, Y_i, Z_i, Z_i^2, Z_i^3) \quad (i \text{ は奇数, かつ } 1 \leq i \leq 2^w-1)$$

をチャドノブスキヤコビアン座標で求め、 kP の計算を、 (k_i-1) 回の2倍点の計算は、請求項1記載の修正ヤコビアン座標 $(X, Y, Z, a*Z^4)$ で行い、 k_i 回目の2倍点の結果は、ヤコビアン座標 (X, Y, Z) で求め、 (X, Y, Z) とテーブルの点 P_i との加算は、請求項1記載の修正ヤコビアン座標 $(X, Y, Z, a*Z^4)$ で求めることを、繰り返すことによって得ることを特徴とした請求項5記載の楕円曲線演算装置としている。

【0032】請求項9では、 p を素数、 k を正整数、有限体 $GF(p)$ 上の楕円曲線を $E: y^2 = x^3 + ax + b$ とし、

$E(GF(p))$ の元 $P = (x, y)$ の冪倍点 $kP = P + \dots + P$ (k 回の加算)

を計算する上記楕円曲線演算装置において、 w を正整数とし、 k を

$$k = 2^k0(2^k1(\dots(2^kwW[v] + W[v-1]) \dots) + W[0])$$

($W[i]$ は奇数、かつ $1 \leq W[i] \leq 2^w-1$) と表すとき、

テーブル

$$iP = P_i = (X_i, Y_i, Z_i, Z_i^2, Z_i^3) \quad (i \text{ は奇数, かつ } 1 \leq i \leq 2^w-1)$$

をチャドノブスキヤコビアン座標で求めるとき、はじめに、 $2P = (x, y)$ をアフィン座標で求めることを特徴とした請求項8記載の楕円曲線演算装置としている。

【0033】請求項10では、 p を素数、 k を正整数、有限体 $GF(p)$ 上の楕円曲線を $E: y^2 = x^3 + ax + b$ とし、

$E(GF(p))$ の元 $P = (x, y)$ の冪倍点 $kP = P + \dots + P$ (k 回の加算)

を計算する上記楕円曲線演算装置において、 w を正整数とし、 k を

$$k = 2^k0(2^k1(\dots(2^kwW[v] + W[v-1]) \dots) + W[0])$$

($W[i]$ は奇数、かつ $1 \leq W[i] \leq 2^w-1$) と表すとき、

テーブル

$$iP = P_i = (X_i, Y_i, Z_i, Z_i^2, Z_i^3) \quad (i \text{ は奇数, かつ } 1 \leq i \leq 2^w-1)$$

をチャドノブスキヤコビアン座標で求めるとき、はじめ

に、 $2P = (x, y)$ をチャドノブスキヤコビアン座標で求めることを特徴とした請求項8記載の楕円曲線演算装置としている

【0034】

【発明の実施の形態】以下、本発明の実施の形態について図を用いて説明する。

【0035】(実施の形態1) 図1は楕円曲線演算装置における修正ヤコビアンによる加算点の方法を示すものである。以下同図を参照しながら加算方法を説明する。

【0036】ここでは、 p を160ビットの素数とし、 $GF(p)$ 上の楕円曲線 $E: y^2 = x^3 + ax + b$ 、その元 $P = (X1, Y1, Z1, a*Z1^4)$ 、 $Q = (X2, Y2, Z2, a*Z2^4)$ ($P \neq Q$) で表すとき、

$$P+Q = R = (X3, Y3, Z3, a*Z3^4)$$

を以下のステップで求める。

【0037】step 1. 中間値の計算

$$U1 = X1*Z2^2, U2 = X2*Z1^2, S1 = Y1*Z2^3,$$

$$S2 = Y2*Z1^3, H = U2 - U1, r = S2 - S1$$

を計算する。

【0038】step 2. $R = (X3, Y3, Z3, a*Z3^4)$ を求める。

$$X3 = -H^3 - 2U1*H^2 + r^2,$$

$$Y3 = -S1*H^3 + r(U1*H^2 - X3),$$

$$Z3 = Z1*Z2*H,$$

$$a*Z3^4 = a(Z3^2)^2$$

(実施の形態2) 図2は楕円曲線演算装置における修正ヤコビアンによる2倍点の方法を示すものである。以下同図を参照しながら加算方法を説明する。

【0039】ここでも実施の形態1と同様に、 p を160ビットの素数とし、 $GF(p)$ 上の楕円曲線 $E: y^2 = x^3 + ax + b$ 、その元 $P = (X1, Y1, Z1, a*Z1^4)$ で表すとき、

$$2P = (X3, Y3, Z3, a*Z3^4)$$

を以下のステップで求める。

【0040】step 1. 中間値の計算

$$S = 4X1*Y1^2, M = 3X1^2 + a*Z1^4, T = -2S + M^2$$

を計算する。

【0041】step 2. $2P = (X3, Y3, Z3, a*Z3^4)$ を求める。

$$X3 = T,$$

$$Y3 = -8Y1^4 + M(S-T),$$

$$Z3 = 2Y1*Z1,$$

$$a*Z3^4 = 2^4*(Y1^4)*(a*Z1^4)$$

上記の実施の形態1、2の計算量について述べる。 $GF(p)$ 上の1回の乗算をMul、逆元演算をInv、2乗算をSqで表す。InvとMulの比率は、実装方法により異なるが、SqとMulの比率は、約 $Sq=0.8Mul$ である。

【0042】実施の形態1、2を用いて楕円曲線上の加算、2倍点を実現すると、加算が13Mul+6Sqで、2倍算は、4Mul+4Sq回で実現できる。加算は、従来から知られているプロジェクトブ座標、ヤコビアン座標、チャド

ノブスキヤコピアン座標に比較すると計算量が多いが、2倍算は、従来の座標系のどれよりも少ない計算量で実現できる。

【0043】楕円曲線の冪倍点 kP ($k=160$ ビット) の演算は、加算に比べ2倍算の繰り返し回数が多い。このため、従来例2にヤコビアン座標の代わりに、実施の形態1、2の修正ヤコビアン座標を用いると、高速化ができる。実際、従来例2が1882Mulで合ったのに対し、実施の形態1、2の修正ヤコビアン座標を適用すると、1722Mulで実現できる。よって、2倍算が高速な修正ヤコビアン座標の効果は大きい。

【0044】(実施の形態3) 図3は本発明の実施の形態3における楕円曲線演算装置の構成を示すものである。

【0045】以下同図を参照しながら実施の形態の手順を説明する。 p を160ビットの素数とし、有限体 $GF(p)$ 上の楕円曲線を E とし、 $E(GF(p))$ の任意の元を P , $k \cdot P$ の計算をする。ここで、 k が従来例2のように、以下で表されているとする。

$$【0046】 k = 2^k0(2^k1(\dots(2^kvW[v] + W[v-1]) \dots) + W[0])$$

step 1. 予備計算テーブルの作成

sP ($s=3, 5, \dots, 15$) をアフィン座標で計算し、予備計算テーブルとする。

【0047】 step 2. kP の計算

T を上位ビットより探索し、ウインドウがある毎に、予備計算テーブルの値(アフィン座標)との加算を修正ヤコビアン座標で求めて、その結果を修正ヤコビアン座標で2冪倍するが、最終結果はヤコビアン座標で得ることを繰り返す。

【0048】すなわち、 $2^kP1 + W[2]P$ を、($P1$ は途中の計算結果で修正ヤコビアン座標)

step 2-1. ($k-1$)回、 $P1$ を修正ヤコビアン座標により2倍算する。

【0049】step 2-2. $2^{(k-1)}P1$ を2倍し、結果をヤコビアン座標で与える。

step 2-3. $W[2]P$ をテーブルから参照する(アフィン座標)

step 2-4. ヤコビアン座標の 2^kP1 とアフィン座標の $W[2]P$ を加算し、結果は修正ヤコビアン座標で与える。

【0050】上記実施の形態3の楕円演算装置は、2倍算においては最も計算量の少ない修正ヤコビアン座標を、加算においては、ヤコビアン座標とアフィン座標の結果を修正ヤコビアン座標で得るといふ混合座標を用いることにより、全体の乗算の回数を減らすことができる。実際、トータル計算量は、 $8Inv+1456Mul$ である。従来例の1882Mulに比較して、 $Inv < 53.3Mul$ であれば実施の形態3の方が高速になる。一般に、 $Inv < 30Mul$ であることより、従来例よりはるかに高速に実現出来る。

【0051】(実施の形態4) 図4は本発明の実施の形

態4における楕円曲線演算装置の構成を示すものである。

【0052】以下同図を参照しながら本実施の形態の手順を説明する。 p を160ビットの素数とし、有限体 $GF(p)$ 上の楕円曲線を E とし、 $E(GF(p))$ の任意の元を P , $k \cdot P$ の計算をする。ここで、 k が従来例2のように以下で表されているとする。

$$【0053】 k = 2^k0(2^k1(\dots(2^kvW[v] + W[v-1]) \dots) + W[0])$$

step 1. 予備計算テーブルの作成

sP ($s=3, 5, \dots, 15$) を、 $2P1$ は、アフィン座標で計算し、 $2P+sP$ をチャドノブスキヤコピアン座標で求めることにより、予備計算テーブルを作成する。

【0054】(予備計算テーブルはチャドノブスキヤコピアン座標)

step 2. kP の計算

T を上位ビットより探索し、ウインドウがある毎に、予備計算テーブルの値(チャドノブスキヤコピアン座標)との加算を修正ヤコビアン座標で求めて、その結果を修正ヤコビアン座標で2冪倍するが、最終結果はヤコビアン座標で得ることを繰り返す。

【0055】すなわち、 $2^kP1 + W[2]P$ を、($P1$ は途中の計算結果で修正ヤコビアン座標)

step 2-1. ($k-1$)回、 $P1$ を修正ヤコビアン座標により2倍算する。

【0056】step 2-2. $2^{(k-1)}P1$ を2倍し、結果をヤコビアン座標で与える。

step 2-3. $W[2]P$ をテーブルから参照する(チャドノブスキヤコピアン座標)

step 2-4. ヤコビアン座標の 2^kP1 とチャドノブスキヤコピアン座標の $W[2]P$ を加算し、結果は修正ヤコビアン座標で与える。

【0057】上記実施の形態4の楕円演算装置は、2倍算においては最も計算量の少ない修正ヤコビアン座標を、加算においては、ヤコビアン座標とチャドノブスキヤコピアン座標の結果を修正ヤコビアン座標で得るといふ混合座標を用いることにより、全体の乗算の回数を減らすことができる。実際、トータル計算量は、 $Inv+1593Mul$ である。従来例の1882Mulに比較して、 $Inv < 289Mul$ であれば実施の形態4の方が高速になる。一般に、 $Inv < 30Mul$ であることより、従来例よりはるかに高速に実現出来る。

【0058】(実施の形態5) 図5は本発明の実施の形態5における楕円曲線演算装置の構成を示すものである。

【0059】以下同図を参照しながら本実施の形態の手順を説明する。 p を160ビットの素数とし、有限体 $GF(p)$ 上の楕円曲線を E とし、 $E(GF(p))$ の任意の元を P , $k \cdot P$ の計算をする。ここで、 k が従来例2のように以下で表されているとする。

【0060】 $k=2^k0(2^k1(\dots(2^kvW[v]+W[v-1])\dots)+W[0])$

step 1. 予備計算テーブルの作成

sP (s=3, 5, ..., 15) を、チャドノブスキヤコビアン座標で求めることにより、予備計算テーブルを作成する。

【0061】 (予備計算テーブルはチャドノブスキヤコビアン座標)

step2. kP の計算

T を上位ビットより探索し、ウィンドウがある毎に、予備計算テーブルの値(チャドノブスキヤコビアン座標)との加算を修正ヤコビアン座標で求めて、その結果を修正ヤコビアン座標で2乗倍するが、最終結果はヤコビアン座標で得ることを繰り返す。

【0062】 すなわち、 $2^kP1 + W[2]P$ を、(P1は途中の計算結果で修正ヤコビアン座標)

step 2-1. (k-1)回、P1を修正ヤコビアン座標により2倍算する。

【0063】 step 2-2. $2^{k-1}P1$ を2倍し、結果をヤコビアン座標で与える。

step 2-3. $W[2]P$ をテーブルから参照する(チャドノブスキヤコビアン座標)

step 2-4. ヤコビアン座標の 2^kP1 とチャドノブスキヤコビアン座標の $W[2]P$ を加算し、結果は修正ヤコビアン座標で与える。

【0064】 上記実施の形態5の楕円演算装置は、2倍

算においては最も計算量の少ない修正ヤコビアン座標を、加算においては、ヤコビアン座標とチャドノブスキヤコビアン座標の結果を修正ヤコビアン座標で得るという混合座標を用いることにより、全体の乗算の回数を減らすことができる。実際、トータルの計算量は、1619Mu lである。従来例の1882Mu lに比較して、はるかに高速に実現出来る。

【0065】

【発明の効果】 以上に説明したように本発明は、従来例における問題点を鑑みて行なわれたもので、高速な暗号方式や署名方式を可能にする楕円曲線演算装置を提供することができ、その実用的価値は大きい。

【図面の簡単な説明】

【図1】 本発明における実施の形態1の楕円曲線演算装置の構成図

【図2】 本発明における実施の形態2の楕円曲線の演算装置の構成図

【図3】 本発明における実施の形態3の楕円曲線演算装置の構成図

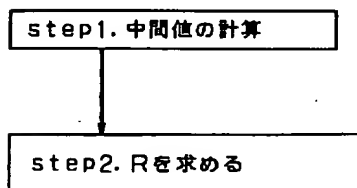
【図4】 本発明における実施の形態4の楕円曲線の演算装置の構成図

【図5】 本発明における実施の形態5の楕円曲線演算装置の構成図

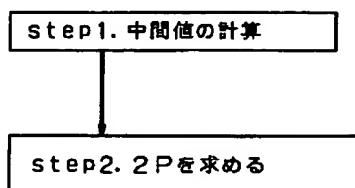
【図6】 従来例1のエルガマル署名の構成図

【図7】 従来例2の楕円曲線演算装置を示す図

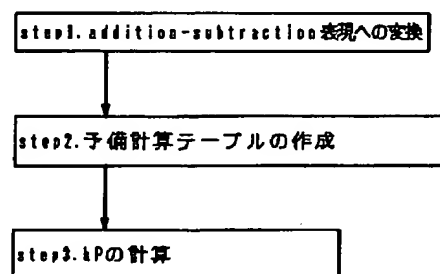
【図1】



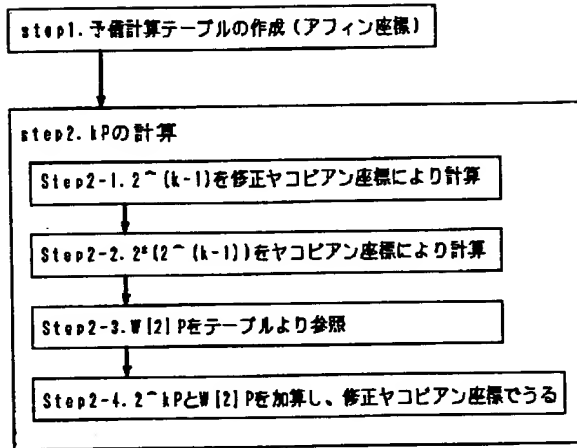
【図2】



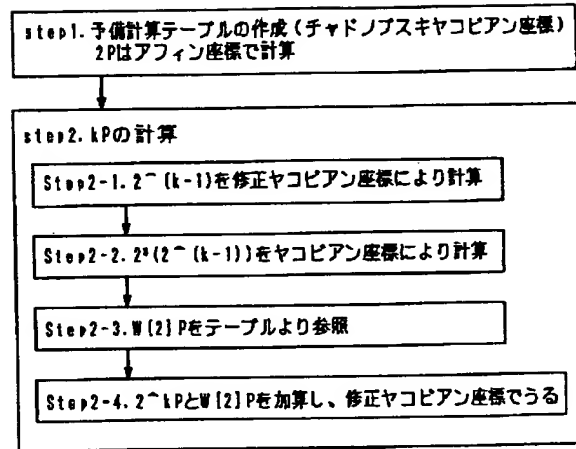
【図7】



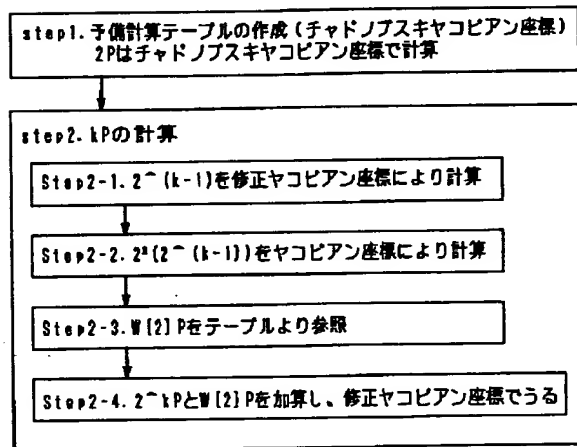
【図 3】



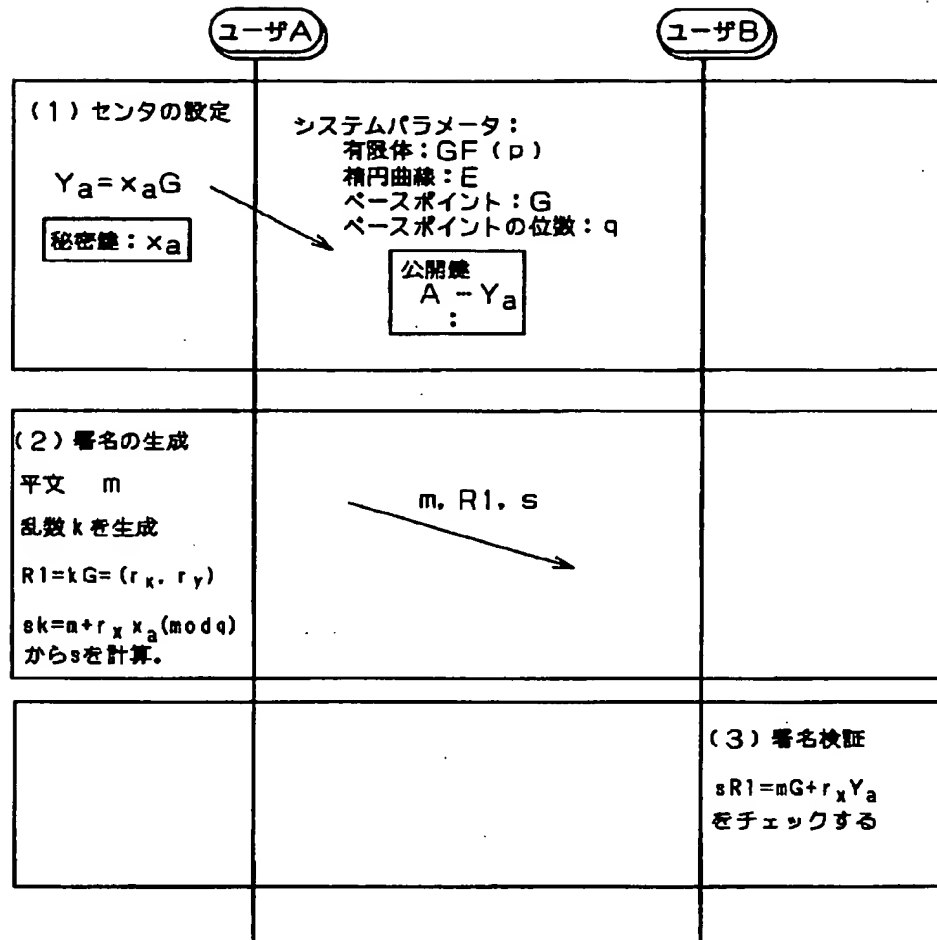
【図 4】



【図 5】



【図 6】



THIS PAGE BLANK (USPTO)